Chapter 1

Introduction

1.1 General Introduction.

Number Theory is a generous branch of Mathematics that studies the properties of numbers for their own objectives which includes the topics: the study of whole numbers, triangular numbers, prime numbers, Fermat's numbers etc.
In Mathematics, it is very easy to discuss what is true, but it is impossible to explain why it is true and example of such phenomenon is Fermat's Last Theorem. Consider the equation

$$x^n + y^n = z^n \tag{1.1.1}$$

For $n = 1, 2$ one may easily find the solution of equation (1.1.1)
i.e. for $n = 1, x = 1, y = 2, z = 3$ and for $n = 2, x = 3, y = 4, z = 5$
Fermat's Last Theorem [18] states that for an integer $n > 2$, equation (1.1.1) has no positive integer solution and he did not given the proof of the same. Many great mathematicians tried to prove the theorem of Fermat, but in 1995, Andrew Wiles in Princeton proved the same.
Theory of Numbers is mainly divided into following different kinds [53]:

(1) **Elementary Number Theory :** The origin of it is antiquity.

(2) **Algebraic Number Theory :** It is studied with the help of mappings, groups, rings, fields etc.

(3) **Analytic Number Theory:** It uses mathematical analysis i.e. inequalities, derivatives, integrals, residues etc.

(4) **Computational Number Theory :** It relates number theory and computer science.

In this thesis we are focusing on study of some known and new results in Elementary Number Theory which studies the set of positive integers which are also called natural numbers.

From ancient times Mathematicians had divided the natural numbers into different types of numbers some of which are as follows [40]:

Even numbers: $2, 4, 6, 8, \cdots$

Odd numbers: $1, 3, 5, 7, 9, \cdots$

Prime numbers: $2, 3, 5, 7, \cdots$

Composite Numbers: $4, 6, 8, 9, \cdots$

Square numbers: $4, 9, 16, 25, \cdots$

Triangular numbers: $1, 3, 6, 10 \cdots$

Perfect numbers: $6, 28, 496, \cdots$

Fibonacci numbers: $1, 1, 2, 3, 5, 8, \cdots$

There are some standard questions in the theory of numbers like:

Sum of Squares.

Que. Can the sum of two squares be a square ?

The answer to this question is affirmative given by Pythagoras (569-470 B.C.) to the western world. Pythagoras theorem [44] states that, there is a triangle [65]with sides x, y and z, that satisfies the equation $x^2 + y^2 = z^2$ which is known as Pythagorean equation. The triple x, y and z of positive integers which satisfies the Pythagorean equation is called Pythagorean triples.

For example: $3^2 + 4^2 = 5^2, 5^2 + 12^2 = 13^2$ etc.

The Pythagorean were the first to give a method of determining infinitely many pythgorean triples [chapter 2, theorem (2.1.2)].

Around 300 B.C. the appearance of Euclid's Elements a collection of 13 books [70]

converted mathematics from numerology into a deductive science [57]. In book X, he gave a method for obtaining all the Pythagorean triples without proof.

[51] gives the relation between primitive Pythagorean triples and Mean Value Theorem. Also [24] discussed the Pythagorean triples whose triangles have a common hypotenuse, inradius, perimeter, area, legsum. Kak [38] and Kothapalli [45] discusses use of primitive Pythagorean triples in cryptography. Roy and Sonia [60] gives a direct method to generate all possible triples both primitive and non-primitive for any given number and developed a technique to produce Pythagorean quadraples and $n-$tuples..

In [67], Pythagorean Triple Metric Sequences are used to shutdown a link. Also [71] disussed the Pythagorean Quadraple.

Triplets of Positive Integers.

Que. Can we find the triplets of positive integers such that sum of any two coordinates is some fixed power ?

We have solved this question in Chapter 3 in details. We have found such triples are infintely many [53], [63]. Arvind [3] found four distinct positive integers such that sum of any two of them is a square.

Number Shapes [21].

The numbers which are arranged in the form of some mathematical figures like triangle, square etc are called the figurate numbers.

The numbers which are arranged in the shape of triangle are called triangular numbers.

For example: $1, 3, 6, 10, \cdots$ are the triangular numbers.

The numbers which are arranged in the shape of squares are called square numbers.

For example: $1, 4, 9, 16, 25, \cdots$ are the square numbers.

The numbers which are arranged in the shape of pentagon are called pentagonal numbers.

For example: $1, 5, 12, 22, 35, \cdots$ are the pentagonal numbers.

Similarly the numbers which are arranged in the shape of Polygon are called polygonal numbers.

A polygonal number denoted by $P_d(n)$ and is a number of the form

$P_d(n) = 1 + [1 + (d-2)] + [1 + 2(d-2)] + \cdots + [1 + (n-1)(d-2)]$

$P_d(n)$ is a d-gonal number of order n [nth d-gonal number].

Que : Is there any relationship between triangular number and other polygonal numbers ?

The answer to this question is also YES.

Every polygonal number can be written in terms of triangular numbers [21]. So triangular numbers plays important role in the study of theory of numbers .

In [25], the relation between Triangular numbers and Prime numbers is discussed in details. Also [32], gives the explanation of writting positive integer in terms of Triangular numbers.

From ancient times, triangular numbers attracts the attention of people all over the world. The interest is not limited to mathematicians and researchers. Further some interesting properties of triangular numbers are found in [49], [58], [33].

Infinitude of primes.

Que. Are there infinitely many prime numbers ?

Que. Are there infinitely many primes that are congruent to 1 modulo 4 and congruent to 3 modulo 4 ?

The answer of these questions is also affirmative. In fact these questions are the particular cases of the well known theorem of the Dirichlet.The infinitude of primes is known from the time of Euclid [56] while the proof of infinitude of primes in terms of arithmatic progression is first given by Dirichlet after the faulty proof given by Legendre.

Dirichlet Theorem:[57] If $a, d \in \mathbb{N}$ and $\gcd(a, d) = 1$, then the infinite sequence $a + d, a + 2d, a + 3d, \cdots$ contains infinitely many primes.

For the proof of theorem , Dirichlet used the complex analysis, so in the history of Number Theory Dirichlet's original proof is considered to be non-elementary and an-

alytic.

From Dirichlet theorem one may easily conclude that,

(i) there are infinitely many prime numbers.

(ii) there are infinitely many primes of the form $4n+1$ and also of the form $4n+3$, [9], [50], [39] etc.

In Chapter 6 we are focusing on the study of Pseudoprimes and some Primality testing.

1.2 Preliminaries

Definition 1.2.1 (**Prime Number).** *A positive integers $p > 1$ with no proper positive factor other than 1 is called a prime number.*

An integer $n > 1$ which is not prime is called a composite number. The set of primes is countably infinite .

Theorem 1.2.1 (**Fundamental Theorem of Arithmatic).** *Every integer $n > 1$ can be wriiten as a product of primes uniquely, with the prime factors in the product in nondecreasing order [9].*

For integers a, b with $a \neq 0$, we say that a is a factor (or divisor) of b if $b = ka$ for some $k \in \mathbb{Z}$ and in this case we write $a|b$. For integer $n > 1$ and integers a, b; we say that a is congurent to b modulo n, denoted by $a \equiv b$(modulo n) if n divides $a - b$. This is an equivalence relation on the set of integers $\mathbb{Z}$ [6].

Result 1.2.1. [34] If $a \equiv b$(mod n) and $c \equiv d$(mod n), then

(i) $a + k \equiv b + k$(mod n), $ak \equiv bk$(mod n) for any $k \in \mathbb{Z}$.

(ii) $a \pm c \equiv b \pm d$(mod n)

(iii) $ac \equiv bd$(mod n)

(iv) $a^k \equiv b^k$(mod n), $ak \equiv bk$(mod nk) for any $k \in \mathbb{N}$

(v) If $k \in \mathbb{Z}$ is a common divisor of a and b with $\gcd(k, n) = 1$, then $\frac{a}{k} \equiv \frac{b}{k} (\text{mod n})$

(vi) If $a \equiv b (\text{mod } n_i)$, $1 \leq i \leq k$, then $a \equiv b (\text{mod N})$ where $N = \text{lcm}\{n_1, n_2, \cdots, n_k\}$.
In particular $a \equiv b (\text{mod } n_1 n_2)$ if $\gcd(n_1, n_2) = 1$, that is n_1, n_2 are relatively prime,
$a \equiv b (\text{mod } n_1 n_2 \cdots n_k)$ if $n_1, n_2, \cdots, n_k$ are pairwise relatively prime.

(vii) If p is a prime and $a^2 \equiv b^2 (\text{mod p})$, then $a \equiv b (\text{mod p})$ or $a \equiv -b (\text{mod p})$.

Result 1.2.2. [50], [41] For $a, b \in \mathbb{Z}$ and integer $n > 1$;
let $a +_n b =$ the least nonnegative remainder when $a + b$ is divided by n,
$a \cdot_n b =$ the least nonnegative remainder when ab is divided by n.
Then for $n > 1, U(n) = \{k \in \mathbb{N} | k < n \text{ and } \gcd(k, n) = 1\}$ is an abelian group under $\cdot_n$ with identity 1 and its order is $\phi(n)$, where ϕ is called Euler's phi function.
For any $a \in \mathbb{Z}$, with $\gcd(a, n) = 1$ we have $r \in U(n)$ such that $a \equiv r (\text{mod n})$. Then we define $o(a)$ as $o(a) = o(r) = k$ is the least positive integer such that $r^k = 1$ (i.e $a^k \equiv r^k \equiv 1 (\text{mod n})$). Clearly $a^{o(a)} \equiv 1 (\text{mod n})$ and $o(a) | \phi(n)$. Note that ϕ is multiplicative and $\phi(p^k) = p^k - p^{k-1}$ for a prime p and $k \in \mathbb{N}$.
A positive integer n is prime iff $\phi(n) = n - 1$.
For a prime p, a is its own inverse in group $U(p)$ iff $a \equiv 1 (\text{mod p})$ or $a \equiv -1 (\text{mod p})$.

Theorem 1.2.2 (Wilson's Theorem). *[47] An integer $n > 1$ is prime iff $(n-1)! \equiv -1 (mod\ n)$.*

Theorem 1.2.3 (Fermat's Little Theorem (FLT)). *[47] If p is a prime, then $a^p \equiv a (mod\ p)$ for all integers a. If $gcd(a, p) = 1$, then $a^{p-1} \equiv 1 (mod\ p)$.*

Converse of FLT is not true for example, $2^{341} \equiv 2 (\text{mod } 341)$ and $341 = 11 \times 31$ which is not prime.

Theorem 1.2.4 (Euler's Theorem). *[40] If integer $n > 1$ and $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 (mod\ n)$.*

Remark 1.2.1 (**Contrapositive of FLT (Primality test)).** For integer $n > 1$, if there exist $a \in \mathbb{N}$ with $a^n \not\equiv a(\text{mod n})$, then n is a composite number.

Example 1.2.1. As $2^{63} = 2^{60} \times 2^3 = (2^6)^{10} \times 8 = (64)^{10} \times 8 \equiv 1^{10} \times 8 \equiv 8(\text{mod } 63)$ i.e. $2^{63} \not\equiv 2(\text{mod } 63)$, so 63 is not prime.
OR As $\gcd(2, 63) = 1$ and $2^{62} \equiv 4(\text{mod } 63)$, i.e $2^{62} \not\equiv 1(\text{mod } 63)$, i.e. $\phi(63) \not\equiv 62$, so 63 is not a prime.

Theorem 1.2.5 (**Chinese Remainder Theorem).** *[39] Let $n_1, n_2, \cdots, n_r \quad (r \geq 2)$ be positive integers that are pairwise relatively prime and their product be N. The system of r simultaneous linear congruences*

$$x \equiv a_1 (mod\ n_1)$$
$$x \equiv a_2 (mod\ n_2)$$
$$.....$$
$$x \equiv a_r (mod\ n_r)$$

has a unique solution (mod N): $x \equiv N_1 x_1 a_1 + N_2 a_2 x_2 + \cdots + N_r a_r x_r (mod\ N)$ where $N_i x_i \equiv 1 (mod\ n_i)$ and $N_i = \dfrac{N}{n_i} \quad (1 \leq i \leq r)$.

Definition 1.2.2 (**Legendre Symbol and Jacobi Symbol).** *[39] Let p be an odd prime, $a \in \mathbb{Z}$ and $p \nmid a$. If $x^2 \equiv a (mod\ p)$ has solution, then we say that a is a quadratic residue (mod p) , otherwise a quadratic nonresidue (mod p).*
There are $\frac{1}{2}(p-1)$ quadratic residues and equally many quadratic nonresidues (mod p). Legendre symbol $(\frac{a}{p})$ is defined as :

$$(\frac{a}{p}) = \begin{cases} 1 & \text{if } a \text{ is quadratic residue (mod p)} \\ -1 & \text{if } a \text{ is quadratic nonresidue (mod p)} \end{cases}$$

Theorem 1.2.6 (**Euler's Criterion).** *[39] $(\dfrac{a}{p}) \equiv a^{\frac{p-1}{2}} (mod\ p)$.*

Properties:[39] Let $a, b \in \mathbb{Z}$ such that $p \nmid ab$ (p an odd prime). Then
(i) $a \equiv b(\text{mod p}) \Rightarrow (\dfrac{a}{p}) = (\dfrac{b}{p})$

(ii)$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

(iii) $(\frac{a^2}{p}) = 1$

(iv)$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$

(v)$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 (\text{mod } 8) \\ -1 & \text{if } p \equiv \pm 3 (\text{mod } 8) \end{cases}$

Let $m = p_1 p_2 \cdots p_r$ where the p_i are odd primes, not necessarily distinct.
Let $\gcd(a, m) = 1$. Let $(\frac{a}{p_i})$ denote the Legendre symbol for each $i, 1 \leq i \leq r$. Then $(\frac{a}{m}) = (\frac{a}{p_1})(\frac{a}{p_2}) \cdots (\frac{a}{p_r})$. Here left side $(\frac{a}{m})$ is Jacobi symbol.
Properties of Jacobi symbols are similar to Legendre symbol.

1.2.1 Taxicab Number [35], [66]

In the history of mathematics there is a illustrious story about the great Indian mathematician Srinivasan Ramanujan. In Cambridge while working with Hardy (1913), Ramanujan was ill and admitted in a hospital at Putney. Hardy came to visit him in a taxicab whose number 1729 was very dull number for him. Actually Ramanujan found that number to be very interesting one. He told that 1729 is the smallest number which can be expressed in two different ways as a sum of two positive cubes. As a result the numbers which are the taxicab numbers are defined as those m for which there are solutions in positive integers to the equation, $m = a^3 + b^3 = c^3 + d^3$ where $\{a, b\} \neq \{c, d\}$.

The nth taxicab number is a positive integer that can be expressed as a sum of two cubes of positive integers in n different ways. The smallest nth taxicab number is denoted by $T_a(n)$.

The concept of second taxicab number was first mentioned in 1657 by Bernard Frenicle de Bersy and was made famous in the early 20th century by a story involving Srinivasa Ramanujan and G. H. Hardy. In 1938, G. H. Hardy and E. M. Wright proved that such numbers exist for all positive integers n, and their proof is easily converted into a program to generate such numbers. However, the proof makes no

claim at all about whether thus generated numbers are the smallest positive and thus it cannot be used to find the actual value of $T_a(n)$.

Following six taxicab (smallest in size) are known [35].

$T_a(1) = 2 = 1^3 + 1^3$

$T_a(2) = 1729 = 1^3 + 12^3 = 9^3 + 10^3$

$T_a(3) = 87539319 = 167^3 + 436^3 = 228^3 + 423^3 = 255^3 + 414^3$

$T_a(4) = 6963472309248 = 2421^3 + 19083^3 = 5436^3 + 18948^3 = 10200^3 + 18072^3 = 13322^3 + 16630^3$

$T_a(5) = 48988659276962496 = 38787^3 + 365757^3 = 107839^3 + 362753^3 = 205292^3 + 342952^3 = 221424^3 + 336588^3 = 231518^3 + 331954^3$

$T_a(6) = 24153319581254312065344 = 582162^3 + 28906206^3 = 3064173^3 + 28894803^3 = 8519281^3 + 28657487^3 = 16218068^3 + 27093208^3 = 17492496^3 + 26590452^3 = 18289922^3 + 26224366^3$

$T_a(2)$ is also known as the Hardy-Ramanujan number. The subsequent taxicab numbers were found with the help of supercomputers. John Leech obtained $T_a(3)$ in 1957. $T_a(4)$ found in 1991 [59]. J. A. Dardis found $T_a(5)$ in 1994 and it was confirmed by David W. Wilson [19] in 1999. In 2003 Calude S.etal found $T_a(6)$ [10]. $T_a(6)$ was announced by Uwe Hollerbach on March 9, 2008. In [14] upper bound for taxicab and cabtaxi numbers are given.

Cubefree number means a positive integer that is not divisible by any p^3 where p is a prime. If a cubefree taxicab number T is written as $T = x^3 + y^3$, then x and y are relatively prime. Among the taxicab numbers $T_a(n), 1 \leq n \leq 6$, only $T_a(1)$ and $T_a(2)$ are cubefree taxicab numbers. The smallest cubefree taxicab number with three representations was discovered by Paul Vojta in 1981 while he was a graduate student. It is

$15170835645 = 517^3 + 2468^3 = 709^3 + 2456^3 = 1733^3 + 2152^3 = 3^2 \times 5 \times 7 \times 31 \times 37 \times 199 \times 211$.

The smallest cubefree taxicab number with four representations was discovered by Staurt Gascoigne and independently by Duncon Moore in 2003. It is

$1801049058342701083 = 92227^3 + 1216500^3 = 136635^3 + 1216102^3 = 341995^3 +$

$1207602^3 = 600259^3 + 1165884^3$.

Positive integers, three representations, not cube free

$87539319 = 436^3 + 167^3 = 423^3 + 228^3 = 44^3 + 255^3 = 3^3 \times 7 \times 31 \times 67 \times 223$

$1148834232 = 1044^3 + 222^3 = 920^3 + 718^3 = 846^3 + 816^3 = 2^3 \times 3^3 \times 7 \times 13 \times 211 \times 277$.

1.3 Structure of the Thesis

1.3.1 Chapterwise Overview.

Chapter 2. Pythagorean Triples

Chapter 2 studies the different properties of primitive Pythagorean triples with its applications to different areas of Mathematics. We also proved some new properties of Pythagorean triples. We have discussed some basics of congruent numbers.

We have also discussed

1) Existence of Pythagorean triples in terms of A. P. and nonexistence in G. P.

2)Nonexistence of Pythagorean triples in terms of Harmonic Progressions

3) Irrationality of some real numbers like $\sqrt{2}, \sqrt{3}, \sqrt{5}, \cdots$ etc with the help of different properties of Pythagorean triples.

For applications of Pythagorean triples one may use [67], [38], [72] and [16].

Chapter 3. Triplets and Sum of its Two Coordinates

In chapter 3, we have found different types of triples of positive integers such that the sum of any two coordinates is a perfect squares, cubes, fourth powers, fifth powers etc. We have discussed the following results in details in this chapter. For the case of perfect squares use [3], [4], [64] .

R1: For determination of distinct $a, b, c \in \mathbb{N}$ with $n \geq 2$, such that $a+b, a+c, b+c$ are nth power of positive integers.

R2: Determination of a triplet (a, b, c) of distinct positive integers such that $|a-b|, |a-c|, |b-c|$ are perfect squares.

These types of triples are arises from Pythagorean triples which we discussed in chapter 2.

R3: Determination of a triplet (a, b, c) of distinct positive integers such that $a+b, a+c, b+c$ are perfect squares.

R4: Triplets with the help of a known triplet.

R5: Triplets from four tuples with the same property.

With the help of the equations

$$a = \frac{1}{2}(r^n + s^n - t^n)$$
$$b = \frac{1}{2}(r^n - s^n + t^n)$$
$$c = \frac{1}{2}(-r^n + s^n + t^n)$$

we have chosen s, t interms of r and found the triplets with sum of any two coordinates is cube, fourth power of positive integers. We have generalised this result for given any positive integer n.

R6: Four tuples of distinct positive integers such that sum of any two of its coordinates is cube of a positive integer.

Also with the help of Taxicab numbers we have found triplets with sum of any two coordinates as cube of a positive integer.

Chapter 4. On Finite Sum of Polynomial Expressions

There are many different techniques to find the value of $\sum_{r=1}^{n} g(r)$ where $g(r)$ is a polynomial in r [30]. We have developed a very simple technique to find the value of $\sum_{r=1}^{n} g(r)$. Knowing the result for higher degree, we have obtained the results for lower degrees by a process like differentiation. These results are also obtained by Newton's forward difference interpolation formula and by using difference operator operation.

In this chapter we have developed different techniques for the study of finite sum of polynomial expressions which are :

1) Integral Technique which a) determines $\sum n^p$ for $p = 1, 2, 3, \cdots$ and

b) determines $\sum g(n)$ when $g(n)$ is a polynomial.

2) Differentiation Techniques to determine $\sum n^p, \quad p \geq 0$.

3) Forward Difference Techniques

With the help of these we have proved the following formulae

a) $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$

b) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$

c) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\dfrac{n(n+1)}{2}\right]^2$

d) $1^4 + 2^4 + 3^4 + \cdots + n^4 = \dfrac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$

e) $1^5 + 2^5 + 3^5 + \cdots + n^5 = \dfrac{n^6}{6} + \dfrac{n^5}{2} + \dfrac{5n^4}{12} - \dfrac{n^2}{12}$

f) $1^6 + 2^6 + 3^6 + \cdots + n^6 = \dfrac{n^7}{7} + \dfrac{n^6}{2} + \dfrac{n^5}{2} - \dfrac{n^3}{6} + \dfrac{n}{42}$ etc .

Chapter 5. Triangular Numbers

Triangular numbers are figurate numbers as they are represented by some fixed geometric patterns.

While it is not known to history about the first inventor of triangular numbers ; it is known that Pythagoras was known about triangular numbers around 496 BCE. The number 153 is the 17th triangular number. Many Christian have a faith in the number 153 as a symbol of Jesus. Where as the number 666 is also mentioned in the New Testament in the Book of Revelation. Also people believe that New Testament book and Book of Revelation were written by same author John Apostle. So Apostle was aware of the triangular numbers. As a result the most earliest records about triangular numbers are found in New Testament book which was written in between 60 and 100 CE [48], [49], [58], [33].

In chapter 5, we have discussed some known properties [44] and also discussed some new properties of triangular numbers.

We have developed some new properties of triangular numbers such as three trian-

gular numbers in terms of Pythagorean triples, the convergence of the series $\sum \frac{1}{t_n^p}$, For $n \geq 2, n^p$ interms of triangular numbers, Finite series $\sum_{r=1}^{n} t_r^p$, Ratio $\frac{t_{an+r}}{t_{bn+r}}$ for $a, b, m, n, r \in \mathbb{N}$, Unit digits of the triangular numbers.

We also made a conjecture for the relation between any two consecutive triangular numbers and prime number.

Chapter 6. On Primality and Pseudoprimes

As compared to composite numbers, prime numbers are rare. Specific composite numbers : pseudoprimes, Carmichael numbers, strong pseudoprimes and Euler pseudoprimes are rare in comparison with prime numbers but each of them are countably infinite. These numbers have some characteristics as primes [11].

Using Fermat's little theorem, pseudoprimes, Carmichael numbers are defined. Using property of prime p : $p|a_1a_2 \Rightarrow p|a_i$ for some a_i, strong pseudoprimes are defined. Using Euler's criterion, for an odd prime p and $\gcd(a,p) = 1; a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\text{mod } p)$, Euler pseudoprimes are defined. One may also see [7], [28].

Chapter 6 is actually review based chapter. We have discussed some known results regarding pseudoprimes, strong pseudoprimes, Euler pseudoprimes, Carmichael numbers and primality testing [69].